试析电力通信网络的安全维护与管理对策

姜　涛
重庆广汇供电服务有限责任公司信息通信分公司　重庆　400000

摘　要：在电网安全生产建设运营过程中，电力通信网络是承载电力生产、运营、管理等业务的基础性网络，涉及调度自动化、电力市场交易、电网生产管理、工程项目施工、物资采购等多种业务的网络支撑体系，唯有电力通信网处于稳定运行状态，其承载的业务流程和设备系统才可以正常工作，电力生产经营管理活动才能常态运转和开展。但就当前的电力通信网络的工作和运行情况来分析，它还是会存在一些的安全风险和问题，风险因素的发生会对电力企业生产经营管理造成实质性的影响。

关键词：电力通信网络；安全维护；管理对策

Analysis of security maintenance and Management Countermeasures of power communication network

Tao Jiang
Chongqing Guanghui power supply service Co., Ltd. information and communication branch, Chongqing 400000

Abstract: in the process of safe production, construction and operation of power grid, power communication network is the basic network carrying power production, operation and management. It is a network support system involving dispatching automation, power market transaction, power grid production management, engineering project construction, material procurement and other businesses. Only when the power communication network is in a stable operation state, its business process and equipment system can work normally, Power production, operation and management activities can be operated and carried out normally. However, based on the analysis of the current work and operation of power communication network, there will still be some security risks and problems. The occurrence of risk factors will have a substantial impact on the production, operation and management of power enterprises.

Keywords: power communication network; Safety maintenance; Management Countermeasures

前言：

从70年代的载波通信，到80年代模拟微波和90年代数字微波，再到如今以光纤通信为主的电力通信网络，随着电力调度自动化业务水平和网络通信技术的不断发展，电力通信网所应用的通信设备系统及其技术也得到了很大提升，相比传统通信网络，如今的光纤通信网络的稳定性和可靠性有了显著提升，目前在运的光传输网和OTN传输网能够满足大多数电力企业的数据传输和业务管理需求。但是，在日常运营过程中，设备故障和安全问题仍存在于这个相对特殊的网络体系当中，我们在提高自动化管理水平的同时，通信网络的设备系统安全、数据信息安全、运行维护安全同样也不容忽视，本文将围绕电力通信网的安全运行维护与管理对策展开深入的讨论与研究。

1、电力通信网络体系组网现状

1.1组网体系结构及分层

在整个电力通信网络体系中，通信设备和系统的种类繁多，不同种类的设备系统生产厂家不同、传输方式不同、传输容量不同、接口规模不同、设备连接方式以及信息的转换方式也是不同的，从而造成了电力通信网络的结构复杂化、兼容难度大。电力通信网络大多采用双设备覆盖、双上联链路的结构方式，通信数据网络划分为核心层、骨干层和接入层，其组网结构普遍分为水平和垂直两个方向，骨干网、接入网是水平层面的两张网；传输网、数据网、支撑网是垂直分布的三张网。

1.2骨干通信网

垂直分布的传输网、数据网、支撑网共同构建电力通信的骨干网。其中，传输网是数据信息的传输通道，是通信网最底层、最基础的交互网络，它由光缆线路设施和传输设备设施等共同组网实现，为信息和数据传递提供平台和通道；数据网必须建立在传输网的基础之上，它是一张按照相关协议进行数据通信的业务网，通过不同的数据传输技术，根据不同的业务和通信方式，在终端之间进行数据信息传递，就其业务类型的不同可以分为调度数据网、电话交换网、会议系统网、数据通信网、应急通信系统网等；支撑网是传输网和业务网正常运行的保障，为增强通信能力和网络服务质量而形成的专业支撑网，包括电源系统、时钟系统、监控系统、网管系统等。

1.3 接入通信网

电力通信网络的规模大、跨度大、结构复杂，在电力生产发、输、变、配、用的各个环节均涉及电力通信网的承载与支撑，其信息来源广泛而且分散，主要包括生产检修数据、工程施工数据、项目管理数据、信息集采数据、档案资料数据、业务管理数据等。接入网分为输变电通信网与配电通信网，它是骨干网之外到属地终端设备设施之间的网络，相比骨干网其传输容量和网络规模都要小，但其节点数量众多，地域和业务分部范围较广。

2、电力通信网络管理的主要问题

2.1 物理层面的安全问题

电力通信网络在物理层面的安全管理问题屡见不鲜，主要包括以下现象：部分设备投运年限久远，导致备品备件相应资源严重缺乏，为后期故障处理带来隐患；光缆线路日常管理不到位，受施工、偷盗、故意损坏等人为外力因素的破坏导致光路中断的现象依然存在；因自然灾害（雪灾、滑坡、地震、恶劣天气等）等不可抗力因素导致通信光缆破坏光路中断；通信机房运维管理制度执行不到位，导致沟道封堵和机房硬件设施损坏，老鼠或其它小动物进入生产环境破坏线缆设备；机房巡查整改制度执行不严，部分视频监控、安防设施、消防设施、空调设施等硬件环境长期损坏失修，导致机房环境不能满足运行要求；日常通信类施工检修工作的方案审查不严，作业现场的监护管理不到位，作业人员人为勿动误碰设备线缆导致光路中断。

2.2 网络身份认证问题

目前电力通信网的身份认证方式大多采用用户手工输入用户名–密码的口令鉴别方式，这种系统或硬件自带的口令认证模式是一种比较原始落后的身份认证方式，其抗击风险和攻击的能力本身是比较弱的，再加上密码口令监管与更新机制不健全，就会导致系统设备存在弱口令、用户名密码长期更新的情况，长此以往，通信网络的身份认证将形同虚设，无法防范非法用户越限越权操作，无法抵御网络攻击者对网络的非法入侵和攻击破坏，更不能满足当前通信网络的安全管理要求。

2.3 网络结构优化和异构网互联问题

当前的电力通信网络采用SDH光传输、OTN等多种技术体制并存的通信传输模式。社会日益增长的供电需求，促使各地区电厂和变电站新建数量逐年增加，因此并入通信网络拓扑结构的网元设备越来越多，其结构越来越复杂臃肿，并缺乏及时有效的网络优化。异构网管互联互通，不同设备类型统一网格化管理是网管系统发展的一个方向，由于不同厂家设备的生产标准、制造工艺、工作模式、接口类型、管理模式等都是不同的，造成电力通信网络管理系统多元化、复杂化，没有形成统一的管理标准，不能实现统一管理、互联互通。

2.4 数据信息明文存储传输问题

电力的通信网络是在自建的光纤网络环境（以下简称内网）中运行的，与外部互联网可以实现物理隔绝，所以在电力内网设备和系统中存储的数据信息都是以明文形式存在，包括数据信息的传输也是以明文形式进行传输，都未曾进行过加密处理。当前的网络环境越来越复杂，伴随着外部终端系统接入内部网络的情况越来越多，必然导致非法入侵和攻击愈发增多，数据信息以明文形式存储传输必然存在较大的安全风险。数据信息传输过程中，一旦有非法用户攻入内网，将会对传输数据随意截取或篡改，造成数据泄露失真，甚至可能投放和传播病毒，造成网络瘫痪，这严重影响了网络传输通道的安全性、可靠性及稳定性。

2.5 网络设备运行管理与漏洞扫描问题

电力通信网络环境中的设备硬件及系统种类繁杂，有国内产的，也国外产的；有同类型同标准的，也有异构特殊的，任何的网络设备系统都可能存在安全漏洞和后门，如果非法入侵者获取了相关漏洞和后门的信息，就会利用各种攻击程序和手段进行网络入侵和攻击，轻者造成传输信息被篡改失真，重者可能导致通信中断、网络瘫痪。随着电力行业信息化进程不断推进，其通信网络的规模和复杂性日益扩大，目前各公司管理的信息网络设备数量众多，种类繁多，存在设备漏洞扫描不及时、不全面的问题。另外，外部终端系统接入内部网络

的情况越来越多，导致网络安全监视管理的压力越来越大。再者，部分企业管理者或网络管理者的安全防范意识不强，不屑于进行网络防护系统的升级改造完善。以上情况都会加大网络干扰、攻击、入侵的几率。

2.6 网络终端设备及用户的安全管理问题

电力系统中，网络终端设备和网络用户管理也是信息安全管理的难点，电力通信终端虽然用户单一，但是用户和终端的数量较多且地域分散，部分网络用户安全意识淡薄，综合素质能力有待提高，不能适应安全管理的要求。目前，通信技术正在飞速的进步发展，如果企业单位不紧跟技术更新的步伐，只是拘泥于相关规则和标准规范中，没有超前学习和创新意识，不去广泛提高干部员工的安全思想意识和综合素质，可能会频繁出现违规操作现象，从而为网络安全监管埋下隐患。

3、常用的网络安全防护技术分析

3.1 网络防火墙技术

网络防火墙是一种特殊的网络访问控制设备，是一道介于企业内部网络和外部网络之间的安全屏障，能够协助网络管理者对网络安全风险进行全方位的监测和管理，其工作原理是利用预先设定的网络安全策略对非法数据传递和接口访问进行甄别和筛选，如遇到病毒入侵和外界攻击，防火墙能够主动发挥监测保护功能，阻绝屏蔽非法入侵。应用级网关防火墙、网络边界防火墙、监测型防火墙等各类型防火墙广泛应用于信息通信网络中，通过网络安全规划，正确有效的部署实施在网络各应用层级，能够有效保障网络环境安全和数据访问安全。

3.2 病毒防护技术

因为网络病毒存在强大的破坏力，必须对病毒的传播加以必要的防护。目前常用的技术方法主要有基于网络安全目录和文档的安全保护措施、工作环境占中防病毒芯片的使用、基于网络服务器针对性反病毒技术的应用、反病毒信息技术等，通过相关技术方法的应用部署，在一定程度上能够有效预防病毒。其中，基于网络服务器的反病毒信息技术可以运用于电力通信网安全保护中，其使用了NLM技术，并采用模块化设计的方式对整体程序作出了合理的设计，把网络服务器当作工作基础，及时对外部网络中出现的病毒进行监测扫描，以确保网络服务器不被病毒感染安全稳定的工作运转。在通信网的信息安全保护领域利用病毒防护技术方法加强对网络病毒的监控预防，也是一项十分关键科学的应对策略。

3.3 入侵检测技术

入侵检测技术，是网络设备对关键数据、重要文件、用户操作行为等因素进行分析对比鉴别攻击行为并主动防御告警的监测技术。入侵检测系统最主要的两个检测方面是非法访问行为和系统外部侵入，通过入侵检测系统的安装和应用，可以检测网络中的未经授权行为，加以判断是否符合规定，再结果处理或上报。如果将防火墙技术和入侵检测技术联合应用，可以给系统网络构建一个强大的防护罩，大大降低攻击和入侵概率。电力行业通过入侵检测相关技术的应用，可以实现电力信息数据的标准化、开放化、高效化管理，同时还能增加和外界的信息交流与技术应用，入侵检测技术贯穿在电力系统每个需要安全维护的环节中，它能够有效阻止外部攻击，使电力系统网络安全稳定。

3.4 备份技术

常用的备份方式有定期物理备份、数据库备份、网络数据备份、远程镜像备份等，主要技术包括LAN备份、LAN Free备份和SAN Server-Free备份。生产运营的过程数据资料、重要信息文件、工程数据资料等重要关键数据大都存储在备份设备当中，如果网络硬件设备大规模出现问题，或是受到各种病毒的功击，或是自然不可抗力等因素，整个能源网络系统有可能出现瘫痪风险，进而造成存放在电力存储设备中的重要数据资料直接丢失损失。为了防止此类现象的出现，可以对重要生产数据实时传输及完整备份，实现相关数据零丢失和远程集群支持；也可以进行异地灾备中心建设，在同地和异地实时备份关键数据。

4、电力通信的网络管理特点与安全性分析

4.1 电力通信网络管理要求

（1）网络管理系统功能受电力通信网络的复杂性和多样性技术的影响较大，必须要全面发展革新。从电力通信网络的出现和发展来看，它是一种综合各种技术的网络，而且伴随着网络技术的不断更新发展，随着时间的变化网络管理会越来越复杂，只有网管系统具备更加全面的功能，才可以保证电力通信网络系统的正常稳定发展。

（2）电力通信网是不断改变的。为了能够维护好通信网络系统的可持续性，就需要增强网络系统的适应性。新技术会随着时代和科技的进步而不断涌现，同时网络系统中传输带宽范围、容量系列范围、连接服务类型与环境、地理覆盖区域以及各方面的条件都会发生不同改变。

（3）对用户敏感度较强。由于当前电网调度和其智能化等很多关键的服务都是采用电力通信网络支撑的，

同时用户对于电力通信网络的服务品质需求特别高，有着很大的敏感度，要使网络管理能够很好地满足服务品质的标准和需求，就需要增强网络的实时性有效性和可信度。

4.2 电力通信网络稳定性和安全性分析

（1）违规外联问题。电力行业的内部办公网络和外部互联网可以实现物理隔绝，内部办公网络在自身搭建的光纤网络中运行，其生产所用的内网终端，必须为专机专用，严禁直接或间接接入外部互联网；接入内网的移动存储介质必须经过加密和认证处理，防止非法设备终端或移动介质携带木马病毒或其他不明信息进入内部网络。

（2）服务器正常运行的监控问题。随着计算机应用的技术和应用范围日益扩大，计算机系统提供的相关业务越来越丰富，服务器使用也越来越多，随着服务器群体的日益壮大，对这些服务器运行状况的监测就显得越来越困难。

（3）操作系统补丁管理问题。对操作系统补丁的管理工作是非常有必要性的，同时也是一项绝对不能够忽略的关键工作。如果总是不能制定一套完整的控制系统补丁策略，将会产生非常严重的影响，例如在关键任务当中的生产管理系统将会失效，高安全性的系统将会遭到恶意的使用，从而会造成不必要的损失。

5、电力通信网络管理的构想

5.1 采用TMN的体系结构

随着电力通信网的发展，网管系统在通信网络的运行管理过程中已随处可见，目前的网管系统对网元设备故障的监控功能已经比较完善，但是对设备性能及配置的监控能力还有所欠缺。可利用TMN的体系结构来进行电力通信网的管理，TMN是为电信网络管理而设计的，能够适应多合同、多厂商合作的技术需求，可以保障电力通信网长期稳健发展。其中，TMN包含了信息、功能、Q3标准互联接口和物力资源等多方面的复杂结构系统。

5.2 实现网管系统标准化

由于互联网信息的大力发展，信息化网络和数据资源共享时代已然到来。电力通信网管信息系统在这一大环境下，应当融入更现代化的信息和技术，应该具有统一的管理设计规范及应用接口标准，让通信设备及网络发挥其最大管理效能，不断提升业务管理水平和效率。在目前，通信网络中应用的最普遍的方式是将标准互连接口作为系统互连的限制协议，后期的应用管理可以将标准限制和实际应用二者有效整合到一起。

5.3 实现应用接口的开放性

实现应用接口开放性的前提是先询问应用需求，进而按照应用的实际状况配置了适当的设备，并对其加以保护，从而使得业务应用的功能可以顺利地进行。网管系统除了必须具有供用户使用的基本功能之外，还必须反映出应用功能接口的开放性。因此网管系统应该在保证当前系统能够正常工作的前提下，持续地为应用创新界面和功能，以满足更多要求。

6、解决电力通信网络管理问题的措施

6.1 物理层安全防护综合措施

不断修订完善电力通信网络设备运行维护管理制度，最大限度的控制预防由设备自身因素和人为、动物、自然等外力因素导致的通信网络破坏，采取主要的防范措施如下：（1）定期梳理网内老旧设备，逐年滚动更新换代。（2）架空光缆，选用外护套内含有特殊玻璃纤维结构的光缆或尾纤，防止鼠咬等小规模的外力破坏。（3）完善通信机房的各类管理规范，包含机房出入及安保管理、机房环境及周边巡视巡查管理、空调等配套设施的巡查管理、安防及消防设施的巡检管理等，严格执行相关制度，确保硬件设施安全可靠。（4）加强电力通信施工检修现场的监护监督，防止人为原因勿动误碰设备线缆，导致通信中断。（5）严格执行通信设备及设施的定期巡检制度，及时发现隐患问题，跟踪闭环管理。（6）提前梳理重要光缆、重点场所、重点设备的应急调整方式，对应急方式的可行性保存滚动修编，最大程度提高通信系统应急方式调整效率，以此来应对不可抗力造成的网络破坏。

6.2 保障安全与增强网络运行稳定性的技术措施

为了使电力通信网络更加安全稳定可靠，还可以从以下技术措施入手加强对网络的加固：（1）在网络的关键及重要节点安装防火墙，有效查杀病毒及木马，防止非法入侵和攻击；部署实施分布式入侵检测架构，实时扫描网络中存在的安全漏洞和后门，防止外部入侵和攻击，实现网络运行状态可持续全天候监控。（2）采取专业性较强的文件格式和通信规约，实现数据信息加密存储或传输，利用公开密匙法（不对称加密）对通道中传输的数据和信息进行加密加工。（3）结合电力通信实际，建立合理安全的身份验证与授权机制，可以采用一次性口令、定期更新口令来进行身份验证。（4）对重要及核心数据定期备份冗余，实现异地灾备中心建设，在同地和异地实时备份关键数据。（5）防止内网终端、介质的违规外联现象，设定或限制其互联网功能，预先设置策

略并及时告警，有效的保护内网信息，将非法操作详细记录在案。（6）尽量使用国产化自主核心网络设备终端，逐渐腾退网络中存在的国外在运设备，确保在运网络设备可控、能控、在控。（7）加强虚拟网（VPN）等先进网络技术的应用，实现数据信息点对点安全交互。

6.3 落实电力通信网络安全管理措施

（1）人员的管理。电力通信网的安全保障，需要经常地对电力通信网的管理者进行相应的安全知识的教育，以提升电力信息网的管理者的知识能力，以提高电力信息网管理者的高度责任感。同时，还必须建立规范的有关电力通信网安全管理制度的规定，并且必须做到避免有关工作人员在调离的状况下，出现对网络安全机密的泄漏问题。（2）密码的管理。密钥管理是通信网的安全保护与管理工作措施中，较为关键的。由于如果将电力通信网的秘密全部遗忘了，再把秘密重新找回来的可能性就很小。所以，需要搞好对电力通信网的密码管理，防止默以秘密、出厂秘密或者无秘密的设定，并且需要对秘密实行定期的更新，以防止出现秘密被盗的状况发生。（3）技术的应用。加强新手段、新措施、新技术的网络知识的学习应用，利用网络防火墙、物理隔离设备、入侵检测设备等技术手段来综合有效的管理通信网络。

6.4 实现不同厂商设备的互连互通

首先需要将接入平台的统一合理地处理，而接入平台又需要保证统一性，才能够合理的进行电力通信的“互连”，为了达到各个厂家之间设备运行的相通、互联及互使用这三个层次的统一性，必须得依靠电力通信厂家推出的通讯产品以及具有国际标准连接的运作系统。然后，其管理工作消息的模式必须保证统一性，只要保证好管理信息模型的统一性，才能够达到“相通”；再接着，就必须得在保证好控制信息模块的统一性下，做到了管理服务及其功能的统一性；最后，在以上的基础上，整个电力通信系统才能够做到“互操作”。

7、结束语

总之，要确保电力通信系统网络安全可靠稳定的运行，必须结合生产实际采取科学有效的防护措施和技术手段。本文仅对网络维护与管理中个人认为效果较好的措施和方法进行了简要分析阐述，希望对电力通信网络的安全防护及管理有所帮助。

参考文献：

[1]张一伊.探讨电力通信网中通信电源故障与维护[J].中国新通信，2020，22（07）：10-11.

[2]李伟.电力通信网中通信电源故障处理与维护分析[J].通信电源技术，2019，36（08）：94-95.

[3]曹百慧.电力通信网的安全维护与管理措施[J].数字通信世界，2018，（10）：220.

[4]甘志洲，胡珂珏，向晓萍.电力通信网安全维护与管理对策[J].通讯世界，2018，（09）：85-86.

[5]代诗磊.电力通信网的安全防护措施与需求分析[J].通讯世界，2018，（07）：234-235.

[6]徐春阳.电力通信网的安全维护与管理措施[J].中国高新区，2018，（05）：222.

[7]谢君鹏，赵勇，鲜涛，李一波，雷宇.电力通信网的安全维护与管理措施[J].中国新通信，2018，20（03）：162-163.

[8]慕春芳，粘中元，罗金玉，张海全.蒙东电力中兴传输设备维护研究[J].信息通信，2017，（07）：165-166.